UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/923,075	08/06/2001	Lynn Henry Wheeler	10399-34383	1892

26702 7590 07/14/2005

MORRIS, MANNING & MARTIN LLP
6000 FAIRVIEW ROAD
SUITE 1125
CHARLOTTE, NC 28210

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/923,075	WHEELER ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *12-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *12-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11042002; 11042002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☒ Other: *See Continuation Sheet*.

Continuation of Attachment(s) 6). Other: IDS: 11042002; 08142003; 08182003.

DETAILED ACTION

Claims 12-20 have been considered.

Election/Restrictions

Claims 1-11 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to nonelected groups, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 6/22/05.

Information Disclosure Statement

It should be noted that the applicant has submitted an exorbitant amount of prior art on numerous PTO-1449's which, on initial consideration, do not all appear to have relevancy or pertinence to the instant invention as claimed. The applicant is requested in response to this office action to point out which of these numerous prior art are pertinent or relevant to the patentability of the invention as claimed in this instant application. It should be noted that it would be advantageous to provide a concise explanation of why each of the prior art is being submitted and how it is understood to be relevant. "Concise explanations are helpful to the Office, particularly where documents are lengthy and complex and applicant is aware of a section that is highly relevant to patentability or where a large number of documents are submitted and applicant is aware that one or more are highly relevant to patentability." (See MPEP 609 under subheading "A. CONTENT").

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 12-14 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed to an abstract method which is non-statutory.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 12 and 15-17 rejected under 35 U.S.C. 102(b) as being anticipated by FIPS 186 (Announcing the Standard for Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186, 5-19-94. pages 1-18).

As per claim 12, the applicant describes a method of obtaining a random number for utilization in an application requiring a random number, comprising generating a digital signature using a digital signature algorithm, and then using said generated digital signature as the random number in the application (pages 4-10).

FIPS 186 discloses the well known digital signature algorithm (DSA). Within DSA, a digital signature is generated by a sender. A verification application on the receiving end requires a digital signature, which is a random number, in order to perform calculations to authenticate the sender.

As per claims 15-17, the applicant describes the method of claim 12, which is met by FIPS 186, with the following limitation which is also met by FIPS 186:

Wherein the digital signature is generated within the computer chip using a private key of a public-private key pair and a random number obtained from the random number generator (pages 4-10).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over FIPS 186 in view of Binding, U.S. Patent No. 6,775,772.

As per claim 13, the applicant describes the method of claim 12, which is met by FIPS 186, with the following limitation which is met by Binding:

Further comprising the step of using the digital signature as a random number to safeguard against a replay attack (Col 9, line 64 to Col 10, line 11);

FIPS 186 discloses all the limitations of claim 12. However, FIPS 186 does not disclose that the digital signature can be used to prevent a replay attack. Binding discloses the idea of creating a digital signature over a nonce. By digitally signing a nonce, replay attacks can be prevented because a hacker will not be able to manipulate the nonce without modifying an authenticated digital signature.

Combining Binding with FIPS 186 allows a nonce to be in the digital signed. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Binding with those of FIPS 186 because doing so allows for verification of a digital signature to also prevent replay attacks.

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over FIPS 186 in view of Ellison, U.S. Patent No. 6,073,237.

As per claim 14, the applicant describes the method of claim 12, which is met by FIPS 186, with the following limitation which is met by Ellison:

Further comprising the step of using the digital signature to generate a session key for secure electronic communication (Col 4, lines 62-67);

FIPS 186 discloses all the limitations of claim 12. However, FIPS 186 does not disclose generating a session key. Ellison teaches that a session key is generated only after a successful verification of a digital signature. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Ellison with those of FIPS 186 and generate a session key only after successful verification of a digital signature because doing so increases security in the system because the session key can only be generated after the verification function authenticates a digital signature.

Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over FIPS 186 in view of the applicant's admitted prior art.

As per claim 18, the applicant describes the method of claim 17, which is met by FIPS 186, with the following limitation which is met by applicant's admitted prior art:

Wherein an elliptical curve digital signature algorithm is utilized to generate the digital signature (applicant: [0146]);

FIPS 186 discloses all the limitations of claim 17. However, FIPS 186 does not disclose that the digital signature is created using an elliptical curve digital signature algorithm.

The applicant discloses that using an elliptical curve digital signature algorithm is a common way to generate a digital signature. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of the applicant's admitted prior art with those of FIPS 186 and generate the digital signature using an elliptical curve digital signature algorithm because doing so is a common way of generating a digital signature.

Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over FIPS 186 in view of the applicant's admitted prior art in further view of Wang, U.S. Patent No. 6,594,759.

As per claims 19 and 20, the applicant describes the method of claim 18, which is met by FIPS 186 in view of the applicant's admitted prior art, with the following limitation which is met by Wang:

Wherein the random number generator is directly inaccessible from outside the computer chip (Col 13, line 49 to Col 14, line 6);

FIPS 186 in view of the applicant's admitted prior art discloses all the limitations of claim 18. However, FIPS 186 in view of the applicant's admitted prior art fails to disclose a random number generator being inaccessible from outside the computer chip. Wang discloses using a random number generator in an authentication system similar to that of FIPS 186 in view of applicant's admitted prior art. Wang also discloses that the random number generator can be used solely by a computer chip or by an entire host computer. In the case where the random number generator is accessible only be the computer chip, it is directly inaccessible to the host computer outside the chip.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew B. Smithers

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137